infrastructure we have in the United States today and opened the door for entrepreneurs to make America's internet economy the best in the world, not by using 1934 regulations that probably regulated telegraphs.

This decision will not take away anyone's privacy or hinder their access to the internet. Instead, it will stop the confusion between two governing bodies: the FCC trying to get in on the action of the Federal Trade Commission, which has always governed internet privacy.

This levels the playing field and keeps competition, instead of the censorship we are seeing on the internet by very few providers. I think this opens the door back up for these wrong-headed regulations of 2015, and gives us all more choices.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 4 of rule I, the following enrolled joint resolution was signed by the Speaker on Thursday, December 7, 2017:

H.J. Res. 123, making further continuing appropriations for fiscal year 2018, and for other purposes.

COMMUNICATION FROM THE CLERK OF THE HOUSE

The SPEAKER pro tempore laid before the House the following communication from the Clerk of the House of Representatives:

OFFICE OF THE CLERK,
HOUSE OF REPRESENTATIVES,
Washington, DC, December 11, 2017.

Hon. PAUL D. RYAN,
The Speaker, House of Representatives, Washington, DC.

DEAR MR. SPEAKER: Pursuant to the permission granted in Clause 2(h) of Rule II of the Rules of the U.S. House of Representatives, the Clerk received the following message from the Secretary of the Senate on December 11, 2017, at 9:50 a.m.:

That the Senate agrees to Conference with the House of Representatives H.R. 1.

With best wishes, I am,

Sincerely,

KAREN L. HAAS.

RECESS

The SPEAKER pro tempore. Pursuant to clause 12(a) of rule I, the Chair declares the House in recess until approximately 4:30 p.m. today.

Accordingly (at 2 o'clock and 6 minutes p.m.), the House stood in recess.

□ 1630

AFTER RECESS

The recess having expired, the House was called to order by the Speaker pro tempore (Mr. PALMER) at 4 o'clock and 30 minutes p.m.

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or votes objected to under clause 6 of rule XX.

The House will resume proceedings on postponed questions at a later time.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ACT OF 2017

Mr. MCCAUL. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3359) to amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3359

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity and Infrastructure Security Agency Act of 2017''.

SEC. 2. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—The Homeland Security Act of 2002 is amended by adding at the end the following new title:

''TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

''Subtitle A—Cybersecurity and Infrastructure Security

''SEC. 2201. DEFINITIONS.

''In this subtitle:

''(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given such term in section 2215.

''(2) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 2209.

''(3) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given such term in paragraph (5) of section 102 of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(4) FEDERAL ENTITY.—The term 'Federal entity' has the meaning given such term in paragraph (8) of section 102 of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(5) NON-FEDERAL ENTITY.—The term 'non-Federal entity' has the meaning given such term in paragraph (14) of section 102 of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

''(6) SECTOR-SPECIFIC AGENCY.—The term 'Sector-Specific Agency' means a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

''(7) SHARING.—The term 'sharing' has the meaning given such term in section 2209.

''(8) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

''(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

''(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

''(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

''(D) facilitating information sharing and operational coordination with threat response; and

''(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

''SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

''(a) REDESIGNATION.—

''(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the 'Cybersecurity and Infrastructure Security Agency' (in this subtitle referred to as the 'Agency').

''(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

''(b) DIRECTOR.—

''(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this subtitle referred to as the 'Director'), who shall report to the Secretary.

''(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of the enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of Cybersecurity and Infrastructure Security of the Department.

''(c) RESPONSIBILITIES.—The Director shall—

''(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

''(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

''(3) carry out the Secretary's responsibilities to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

''(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

''(5) upon request provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide such analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

''(6) develop and utilize mechanisms for active and frequent collaboration between the

Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

''(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Agency's Divisions to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

''(8) develop, coordinate, and implement—

''(A) comprehensive strategic plans for the activities of the Agency; and

''(B) risk assessments by and for the Agency;

''(9) carry out emergency communications responsibilities, in accordance with title XVIII;

''(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate such outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; and

''(11) carry out such other duties and powers prescribed by law or delegated by the Secretary.

''(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

''(1) assist the Director in the management of the Agency; and

''(2) report to the Director.

''(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

''(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

''(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies (including law enforcement agencies), and private sector entities, and to integrate such information, in support of the mission responsibilities of the Department, in order to—

''(i) identify and assess the nature and scope of terrorist threats to the homeland;

''(ii) detect and identify threats of terrorism against the United States; and

''(iii) understand such threats in light of actual and potential vulnerabilities of the homeland.

''(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks). At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

''(C) To integrate relevant information, analysis, and vulnerability assessments (regardless of whether such information, analysis, or assessments are provided or produced by the Department) in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

''(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining such information from other Federal Government agencies.

''(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support such systems.

''(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

''(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

''(H) To disseminate, as appropriate, information analyzed by the Department within the Department, to other Federal Government agencies with responsibilities relating to homeland security, and to State, local, tribal, and territorial government agencies and private sector entities with such responsibilities in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.

''(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

''(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

''(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

''(L) To establish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

''(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

''(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

''(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

''(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

''(Q) To carry out requirements of the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate established under subtitle J of title VIII.

''(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1) of this subsection, upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to any such reallocation that such reallocation is necessary for carrying out the activities of the Agency.

''(3) STAFF.—

''(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging its responsibilities under this section.

''(B) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

''(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

''(4) DETAIL OF PERSONNEL.—

''(A) IN GENERAL.—In order to assist the Agency in discharging its responsibilities under this section, personnel of the Federal agencies referred to in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

''(B) AGENCIES SPECIFIED.—The Federal agencies referred to in subparagraph (A) are the following:

''(i) The Department of State.

''(ii) The Central Intelligence Agency.

''(iii) The Federal Bureau of Investigation.

''(iv) The National Security Agency.

''(v) The National Geospatial-Intelligence Agency.

''(vi) The Defense Intelligence Agency.

''(vii) Sector-Specific Agencies.

''(viii) Any other agency of the Federal Government that the President considers appropriate.

''(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of an agency specified in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

''(D) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

''(f) COMPOSITION.—The Agency shall be composed of the following divisions:

''(1) The Cybersecurity Division, headed by an Assistant Director.

''(2) The Infrastructure Security Division, headed by an Assistant Director.

''(3) The Emergency Communications Division under title XVIII, headed by an Assistant Director.

''(g) CO-LOCATION.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence. When establishing such locations, the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

''(h) PRIVACY.—

''(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

''(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

''(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

''(B) assuring that personal information contained in Privacy Act systems of records of the Agency is handled in full compliance with fair information practices as specified in the Privacy Act of 1974;

''(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

''(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

''(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of the enactment of this title, of any other component of the Department or any other Federal department or agency.

''SEC. 2203. CYBERSECURITY DIVISION.

''(a) ESTABLISHMENT.—

''(1) IN GENERAL.—There is established in the Agency a Cybersecurity Division.

''(2) ASSISTANT DIRECTOR.—The Cybersecurity Division shall be headed by an Assistant Director for Cybersecurity (in this subtitle referred to as the 'Assistant Director'), who shall—

''(A) be at the level of Assistant Secretary within the Department;

''(B) be appointed by the President without the advice and consent of the Senate; and

''(C) report to the Director.

''(3) REFERENCE.—Any reference to the Assistant Secretary for Cybersecurity and Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Cybersecurity.

''(b) FUNCTIONS.—The Assistant Director shall—

''(1) direct the cybersecurity efforts of the Agency;

''(2) carry out activities, at the direction of the Director, related to the security of Federal information and Federal information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

''(3) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and

''(4) carry out such other duties and powers as prescribed by the Director.

''SEC. 2204. INFRASTRUCTURE SECURITY DIVISION.

''(a) ESTABLISHMENT.—

''(1) IN GENERAL.—There is established in the Agency an Infrastructure Security Division.

''(2) ASSISTANT DIRECTOR.—The Infrastructure Security Division shall be headed by an Assistant Director of Infrastructure Security (in this section referred to as the 'Assistant Director'), who shall—

''(A) be at the level of Assistant Secretary within the Department;

''(B) be appointed by the President without the advice and consent of the Senate; and

''(C) report to the Director.

''(3) REFERENCE.—Any reference to the Assistant Secretary for Infrastructure Protection in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Infrastructure Security.

''(b) FUNCTIONS.—The Assistant Director shall—

''(1) direct the critical infrastructure security efforts of the Agency;

''(2) carry, at the direction of the Director, the Chemical Facilities Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate established under subtitle J of title VIII or successor program;

''(3) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and

''(4) carry out such other duties and powers as prescribed by the Director.''.

(b) TREATMENT OF CERTAIN POSITIONS.—

(1) UNDER SECRETARY.—The individual serving as the Under Secretary appointed pursuant to section 103(a)(1)(H) of the Homeland Security Act of 2002 (6 U.S.C. 113(a)(1)) of the Department of Homeland Security on the day before the date of the enactment of this Act may continue to serve as the Director of the Cybersecurity and Infrastructure Security Agency of the Department on and after such date.

(2) DIRECTOR FOR EMERGENCY COMMUNICATIONS.—The individual serving as the Director for Emergency Communications of the Department of Homeland Security on the day before the date of the enactment of this Act may continue to serve as the Assistant Director for Emergency Communications of the Department on and after such date.

(3) ASSISTANT SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS.—The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of the enactment of this Act may continue to serve as the Assistant Director for Cybersecurity on and after such date.

(4) ASSISTANT SECRETARY FOR INFRASTRUCTURE SECURITY.—The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of the enactment of this Act may continue to serve as the Assistant Director for Infrastructure Security on and after such date.

(c) REFERENCE.—Any reference to—

(1) the Office of Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Emergency Communications Division; and

(2) the Director for Emergency Communications in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Assistant Director for Emergency Communications.

(d) OVERSIGHT.—The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to Congress, in accordance with the deadlines specified in paragraphs (1) and (2), information on the following:

(1) Not later than 60 days after the date of the enactment of this Act, a briefing on the activities of the Agency relating to the development and use of the mechanisms required pursuant to section 2202(c)(6) of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(2) Not later than one year after the date of the enactment of this Act, a briefing on the activities of the Agency relating to its use and improvement of the mechanisms required pursuant to section 2202(c)(6) of the Homeland Security Act of 2002 and how such activities have impacted coordination, situational awareness, and communications with Sector-Specific Agencies.

(3) Not later than 90 days after the date of the enactment of this Act, information on the Agency's mechanisms for regular and ongoing consultation and collaboration, as required pursuant to section 2202(c)(7) of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(4) Not later than one year after the date of the enactment of this Act, the activities of the Agency's consultation and collaboration mechanisms as required pursuant to section 2202(c)(7) of the Homeland Security Act of 2002, and how such mechanisms have impacted operational coordination, situational awareness, and integration across the Agency.

(e) CYBER WORKFORCE.—Not later than 90 days after the date of the enactment of this subtitle, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to Congress a report detailing how the Agency is meeting legislative requirements under the Cybersecurity Workforce Assessment Act (Public Law 113–246) and the Homeland Security Cybersecurity Workforce Assessment Act (enacted as section 4 of the Border Patrol Agent Pay Reform Act of 2014; Public Law 113–277) to address cyber workforce needs.

(f) FACILITY.—Not later than 180 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall report to Congress on the most efficient and effective methods of consolidating Agency facilities, personnel, and programs to most effectively carry out the Agency's mission.

(g) CONFORMING AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002.—The Homeland Security Act of 2002 is amended—

(1) in title I, by amending subparagraph (H) of section 103(a)(1) (6 U.S.C. 113(a)(1)) to read as follows:

''(H) A Director of the Cybersecurity and Infrastructure Security Agency.'';

(2) in title II (6 U.S.C. 121 et seq.)—

(A) in the title heading, by striking ''**AND INFRASTRUCTURE PROTECTION**'';

(B) in the subtitle A heading, by striking ''**and Infrastructure Protection**'';

(C) in section 201 (6 U.S.C. 121)—

(i) in the section heading, by striking ''**AND INFRASTRUCTURE PROTECTION**'';

(ii) in subsection (a)—

(I) in the heading, by striking ''AND INFRASTRUCTURE PROTECTION''; and

(II) by striking ''and an Office of Infrastructure Protection'';

(iii) in subsection (b)—

(I) in the heading, by striking ''AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION''; and

(II) by striking paragraph (3);

(iv) in subsection (c)—

(I) by striking ''and infrastructure protection''; and

(II) by striking ''or the Assistant Secretary for Infrastructure Protection, as appropriate'';

(v) in subsection (d)—

(I) in the heading, by striking ''AND INFRASTRUCTURE PROTECTION'';

(II) in the matter preceding paragraph (1), by striking ''and infrastructure protection'';

(III) by striking paragraphs (5) and (6) and redesignating paragraphs (7) through (26) as paragraphs (5) through (24), respectively;

(IV) by striking paragraph (23), as so redesignated; and

(V) by redesignating paragraph (24), as so redesignated, as paragraph (23);

(vi) in subsection (e)(1), by striking ''and the Office of Infrastructure Protection''; and

(vii) in subsection (f)(1), by striking ''and the Office of Infrastructure Protection'';

(D) in section 204 (6 U.S.C. 124a)—

(i) in subsection (c)(1), in the matter preceding subparagraph (A), by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(ii) in subsection (d)(1), in the matter preceding subparagraph (A), by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency'';

(E) in subparagraph (B) of section 210A(c)(2) (6 U.S.C. 124h(c)(2)), by striking ''Office of Infrastructure Protection'' and inserting ''Cybersecurity and Infrastructure Security Agency'';

(F) by transferring section 210E (6 U.S.C. 124) to appear after section 2213 (as redesignated by subparagraph (H) of this paragraph) and redesignating such section 210E as section 2214;

(G) in subtitle B, by redesignating sections 211 through 215 (6 U.S.C. 101 note through 134) as sections 2221 through 2225, respectively, and inserting such redesignated sections, including the enumerator and heading of subtitle B (containing such redesignated sections), after section 2214, as redesignated by subparagraph (F) of this paragraph; and

(H) by redesignating sections 223 through 230 (6 U.S.C. 143 through 151) as sections 2205 through 2213, respectively, and inserting such redesignated sections after section 2204, as added by this Act;

(3) in title III, in paragraph (3) of section 302 (6 U.S.C. 182), by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency'';

(4) in title V—

(A) in section 514 (6 U.S.C. 321c), by—

(i) striking subsection (b); and

(ii) redesignating subsection (c) as subsection (b);

(B) in section 523 (6 U.S.C. 321l)—

(i) in subsection (a), in the matter preceding paragraph (1), by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(ii) in subsection (c), by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(C) in section 524(a)(2)(B) (6 U.S.C. 321m(a)(2)(B)), in the matter preceding clause (i)—

(i) by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(ii) by striking ''of the Assistant Secretary'' and inserting ''of the Director'';

(5) in title VIII, in section 899B(a) (6 U.S.C. 488a(a)), by inserting at the end the following new sentence: ''Such regulations shall be carried out by the Cybersecurity and Infrastructure Security Agency.'';

(6) in title XVIII (6 U.S.C. 571 et seq.)—

(A) in section 1801 (6 U.S.C. 571)—

(i) in the section heading, by striking ''**OFFICE OF EMERGENCY COMMUNICATIONS**'' and inserting ''**EMERGENCY COMMUNICATIONS DIVISION**'';

(ii) in subsection (a)—

(I) by striking ''Office of Emergency Communications'' and inserting ''Emergency Communications Division''; and

(II) by adding at the end the following new sentence: ''The Division shall be located in the Cybersecurity and Infrastructure Security Agency.'';

(iii) by amending subsection (b) to read as follows:

''(b) ASSISTANT DIRECTOR.—The head of the office shall be the Assistant Director for Emergency Communications. The Assistant Director shall report to the Director of the Cybersecurity and Infrastructure Security Agency. All decisions of the Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director.'';

(iv) in subsection (c)—

(I) in the matter preceding paragraph (1), by inserting ''Assistant'' before ''Director'';

(II) in paragraph (14), by striking ''and'' at the end;

(III) by redesignating paragraph (15) as paragraph (16); and

(IV) by inserting after paragraph (14) the following new paragraph:

''(15) fully participate in the mechanisms required under subsection (c)(7) of section 2202; and'';

(v) in subsection (d), by inserting ''Assistant'' before ''Director''; and

(vi) in subsection (e), in the matter preceding paragraph (1), by inserting ''Assistant'' before ''Director'';

(B) in sections 1802 through 1805 (6 U.S.C. 575), by striking ''Director for Emergency Communications'' each place it appears and inserting ''Assistant Director for Emergency Communications'';

(C) in section 1809 (6 U.S.C. 579)—

(i) by striking ''Director for Emergency Communications'' and inserting ''Assistant Director for Emergency Communications''; and

(ii) by striking ''Office of Emergency Communications'' each place it appears and inserting ''Emergency Communications Division''; and

(D) in section 1810 (6 U.S.C. 580)—

(i) in subsection (a)(1), by striking ''Director of the Office of Emergency Communications (referred to in this section as the 'Director')'' and inserting ''Assistant Director for the Emergency Communications Division (referred to in this section as the 'Assistant Director')'';

(ii) in subsection (c), by striking ''Office of Emergency Communications'' and inserting ''Emergency Communications Division''; and

(iii) by striking ''Director'' each place it appears and inserting ''Assistant Director'';

(7) in title XXI (6 U.S.C. 621 et seq.)—

(A) in section 2101 (6 U.S.C. 621)—

(i) by redesignating paragraphs (4) through (14) as paragraphs (5) through (15), respectively; and

(ii) by inserting after paragraph (3) the following new paragraph:

''(4) the term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency;'';

(B) in paragraph (1) of section 2102(a) (6 U.S.C. 622(a)), by inserting at the end the following new sentence: ''Such Program shall be located in the Cybersecurity and Infrastructure Security Agency.''; and

(C) in paragraph (2) of section 2104(c) (6 U.S.C. 624(c)), by striking ''Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(8) in title XXII, as added by this Act—

(A) in section 2205, as so redesignated, in the matter preceding paragraph (1), by striking ''Under Secretary appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency'';

(B) in section 2206, as so redesignated, by striking ''Assistant Secretary for Infrastructure Protection'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency'';

(C) in section 2209, as so redesignated—

(i) by striking ''Under Secretary appointed under section 103(a)(1)(H)'' each place it appears and inserting ''Director of the Cybersecurity and Infrastructure Security Agency'';

(ii) in subsection (b), by adding at the end the following new sentences: ''The Center shall be located in the Cybersecurity and Infrastructure Security Agency. The head of the Center shall report to the Assistant Director for Cybersecurity.''; and

(iii) in subsection (c)(11), by striking ''Office of Emergency Communications'' and inserting ''Emergency Communications Division'';

(D) in section 2210, as so redesignated—

(i) by striking ''section 227'' each place it appears and inserting ''section 2209''; and

(ii) in subsection (c)—

(I) by striking ''Under Secretary appointed under section 103(a)(1)(H)'' and inserting ''Director of the Cybersecurity and Infrastructure Security Agency''; and

(II) by striking ''section 212(5)'' and inserting ''section 2225(5)'';

(E) in subsection (b)(2)(A) of section 2211, as so redesignated, by striking ''section 227'' and inserting ''section 2209'';

(F) in section 2212, as so redesignated, by striking ''section 212(5)'' and inserting ''section 2225(5)''; and

(G) in section 2213, as so redesignated, in subsection (a)—

(i) in paragraph (3), by striking ''section 228'' and inserting ''section 2210''; and

(ii) in paragraph (4), by striking ''section 227'' and inserting ''section 2209''.

(h) CONFORMING AMENDMENT TO TITLE 5, UNITED STATES CODE.—Section 5314 of title 5, United States Code, is amended by inserting after ''Under Secretaries, Department of Homeland Security.'' the following new item:

''Director, Cybersecurity and Infrastructure Security Agency.''.

(i) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended—

(1) in title II—

(A) in the item relating to the title heading, by striking ''AND INFRASTRUCTURE PROTECTION'';

(B) in the item relating to the heading of subtitle A, by striking ''and Infrastructure Protection'';

(C) in the item relating to section 201, by striking ''and Infrastructure Protection'';

(D) by striking the item relating to section 210E;

(E) by striking the items relating to subtitle B of title II; and

(F) by striking the items relating to section 223 through section 230;

(2) in title XVIII, by amending the item relating to section 1801 to read as follows:

''Sec. 1801. Emergency Communications Division.''; and

(3) by adding at the end the following new items:

''TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

''Subtitle A—Cybersecurity and Infrastructure Security

''Sec. 2201. Definitions.
''Sec. 2202. Cybersecurity and Infrastructure Security Agency.
''Sec. 2203. Cybersecurity Division.
''Sec. 2204. Infrastructure Security Division.
''Sec. 2205. Enhancement of Federal and non-Federal cybersecurity.
''Sec. 2206. Net guard.
''Sec. 2207. Cyber Security Enhancement Act of 2002.
''Sec. 2208. Cybersecurity recruitment and retention.
''Sec. 2209. National cybersecurity and communications integration center.

''Sec. 2210. Cybersecurity plans.
''Sec. 2211. Cybersecurity strategy.
''Sec. 2212. Clearances.
''Sec. 2213. Federal intrusion detection and prevention system.
''Sec. 2214. National Asset Database.
''Subtitle B—Critical Infrastructure Information
''Sec. 2221. Short title.
''Sec. 2222. Definitions.
''Sec. 2223. Designation of critical infrastructure protection program.
''Sec. 2224. Protection of voluntarily shared critical infrastructure information.
''Sec. 2225. No private right of action.''.

SEC. 3. TRANSFER OF OTHER ENTITIES.

(a) OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.—The Office of Biometric Identity Management of the Department of Homeland Security located in the National Protection and Programs Directorate of the Department of Homeland Security on the day before the date of the enactment of this Act is hereby transferred to the Management Directorate of the Department.

(b) FEDERAL PROTECTIVE SERVICE.—The Secretary of Homeland Security is authorized to transfer the Federal Protective Service, as authorized under section 1315 of title 40, United States Code, to any component, directorate, or other office of the Department of Homeland Security that the Secretary determines appropriate.

SEC. 4. RULE OF CONSTRUCTION.

Nothing in this Act may be construed as—

(1) conferring new authorities to the Secretary of Homeland Security, including programmatic, regulatory, or enforcement authorities, outside of the authorities in existence on the day before the date of the enactment of this Act;

(2) reducing or limiting the programmatic, regulatory, or enforcement authority vested in any other Federal agency by statute; or

(3) affecting in any manner the authority, existing on the day before the date of the enactment of this Act, of any other Federal agency or component of the Department of Homeland Security.

SEC. 5. PROHIBITION ON ADDITIONAL FUNDING.

No additional funds are authorized to be appropriated to carry out this Act or the amendments made by this Act. This Act and such amendments shall be carried out using amounts otherwise authorized.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. MCCAUL) and the gentlewoman from California (Ms. BARRAGÁN) each will control 20 minutes.

The Chair recognizes the gentleman from Texas.

GENERAL LEAVE

Mr. MCCAUL. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days within which to revise and extend their remarks and to include any extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. MCCAUL. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of the Cybersecurity and Infrastructure Security Agency Act.

Mr. Speaker, with each passing day, nation-states, hackers, and other cyber criminals are finding new ways to attack our cyber infrastructure and expose new vulnerabilities.

As technology has advanced, more and more Americans have become dependent on computer networks and information technology, making everyone a potential victim.

In September, we learned that Equifax had been successfully hacked and 145.5 million people were affected by this breach. Last month, it is reported that 57 million people who use Uber might have had their personal information stolen in a cyber attack in 2016.

These attacks are not just aimed at American consumers, however. Our foreign adversaries are routinely engaging in cyber warfare as well.

In 2015, hackers traced back to the Chinese Government accessed sensitive material from the Office of Personnel Management on 22 million persons' security clearances. Last year, Russia was caught trying to undermine our democratic process.

These kinds of attacks are simply unacceptable. We must not allow them to continue. Fortunately, we have prioritized cybersecurity issues at the Committee on Homeland Security over the last few years and have taken strong, bipartisan action. In 2014, committee efforts resulted in the enactment of legislation that provided DHS expedited hiring authority, ensuring the DHS is assessing its cybersecurity workforce, and it clarified the Department's role in the cybersecurity of Federal networks.

In 2015, the Cybersecurity Act provided liability protections for public-to-private and private-to-private cyber threat information sharing. While these are important actions, we need to do more, and today we have a chance to do just that.

The legislation before us streamlines the infrastructure of the National Protection and Programs Directorate and redesignates it as the Cybersecurity and Infrastructure Security Agency. This realignment will achieve the DHS' goal of creating a stand-alone operational organization, focusing on and elevating the vital cybersecurity mission of the Department.

This bill requires the appointment of a Director who is responsible for leading cybersecurity and infrastructure programs and operations for the agency, developing and utilizing mechanisms for active and frequent collaboration with sector-specific agencies, and coordinating and implementing comprehensive strategic plans and risk assessments for the agency.

This action enjoys great support from the DHS. Less than two weeks ago, while addressing cybersecurity issues in testimony before our committee, then-Acting Secretary Elaine Duke stated: ''In the face of these digital threats, it is a DHS priority to work with Congress on legislation that would focus our cybersecurity and critical infrastructure mission at the NPPD.''

Taking action today reaffirms that priority.

Cybersecurity is an issue that transcends partisan politics. In light of the risk and potential consequence of cyber attacks, we must stand together and strengthen the security of digital America and the resilience of our cyber networks.

I would like to thank the members of the Homeland Security Committee, Ranking Member THOMPSON, and the staff for all their hard work.

I would also like to thank the Energy and Commerce Committee chairman, Mr. WALDEN; the Transportation and Infrastructure Committee chairman, Mr. SHUSTER; and the Oversight and Government Reform Committee chairman, Mr. GOWDY, for their efforts to see this through.

Mr. Speaker, this is another bipartisan example of how varied stakeholders can come together and draft and pass important legislation. It is an opportunity we have today to elevate the importance of cybersecurity at the Department of Homeland Security to achieve its goal of protecting the United States. I urge my colleagues to support this vital piece of legislation.

Mr. Speaker, I reserve the balance of my time.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, December 8, 2017.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I am writing to notify you that the Committee on Energy and Commerce will forgo action on H.R. 3359, Cybersecurity and Infrastructure Security Agency Act of 2017, so that it may proceed expeditiously to the House floor for consideration. This is done with the understanding that the Committee's jurisdictional interests over this and similar legislation are in no way diminished or altered. In addition, the Committee reserves the right to seek conferees on H.R. 3359 and expects your support when such a request is made.

Please include a copy of this letter outlining our mutual understanding with respect to H.R. 3359 in the Congressional Record during consideration of the bill on the House floor.

Sincerely,

GREG WARDEN,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, December 7, 2017.

Hon. GREG WALDEN,
Chairman, Committee on Energy and Commerce, Washington, DC.

DEAR CHAIRMAN WALDEN: Thank you for your letter regarding H.R. 3359, the ''Cybersecurity and Infrastructure Security Agency Act of 2017.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Energy and Commerce will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Energy and Commerce does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee.

I will insert copies of this exchange in the report on the bill and in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC, December 7, 2017.

Hon. MICHAEL T. MCCAUL,
Chairman, Committee on Homeland Security, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: I write concerning H.R. 3359, the ''Cybersecurity and Infrastructure Security Agency Act of 2017.'' This bill would amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and contains provisions within the jurisdiction of the Committee on Oversight and Government Reform. As a result of your having consulted with me concerning the provisions of the bill that fall within our Rule X jurisdiction, I agree to forgo consideration of the bill, so the bill may proceed expeditiously to the House floor.

The Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 3359 at this time we do not waive any jurisdiction over the subject matter contained in this or similar legislation, and we will be appropriately consulted and involved as the bill or similar legislation moves forward so that we may address any remaining issues that fall within our Rule X jurisdiction. Further, I request your support for the appointment of conferees from the Committee on Oversight and Government Reform during any House-Senate conference convened on this or related legislation.

Finally, I would appreciate your response to this letter confirming this understanding and ask that a copy of our exchange of letters on this matter be included in the bill report filed by the Committee on Homeland Security, as well as in the Congressional Record during floor consideration thereof.

Sincerely,

TREY GOWDY.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, December 7, 2017.

Hon. TREY GOWDY,
Chairman, Committee on Oversight and Government Reform, Washington, DC.

DEAR CHAIRMAN GOWDY: Thank you for your letter regarding H.R. 3359, the ''Cybersecurity and Infrastructure Security Agency Act of 2017.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Oversight and Government Reform will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Oversight and Government Reform does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee.

I will insert copies of this exchange in the report on the bill and in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

HOUSE OF REPRESENTATIVES, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
Washington, DC, December 7, 2017.

Hon. MICHAEL MCCAUL,
Chairman, Committee on Homeland Security, Washington, DC.

DEAR CHAIRMAN MCCAUL: I write concerning H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017. This legislation includes matters that fall within the Rule X jurisdiction of the Committee on Transportation and Infrastructure.

I recognize and appreciate your desire to bring this legislation before the House of Representatives in an expeditious manner, and accordingly, the Committee on Transportation and Infrastructure will forego action on the bill. However, this is conditional on our mutual understanding that foregoing consideration of the bill does not prejudice the Committee with respect to the appointment of conferees or to any future jurisdictional claim over the subject matters contained in the bill or similar legislation that fall within the Committee's Rule X jurisdiction. Further, this is conditional on our understanding that mutually agreed upon changes to the legislation will be incorporated into the bill prior to floor consideration. Lastly, should a conference on the bill be necessary, I request your support for the appointment of conferees from the Committee on Transportation and Infrastructure during any House-Senate conference convened on this or related legislation.

I would ask that a copy of this letter and your response acknowledging our jurisdictional interest as well as the mutually agreed upon changes to be incorporated into the bill be included in the Congressional Record during consideration of the measure on the House floor, to memorialize our understanding.

I look forward to working with the Committee on Homeland Security as the bill moves through the legislative process.

Sincrerely,

BILL SHUSTER,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC, December 7, 2017.

Hon. BILL SHUSTER,
Chairman, Committee on Transportation and Infrastructure, Washington, DC.

DEAR CHAIRMAN SHUSTER: Thank you for your letter regarding H.R. 3359, the ''Cybersecurity and Infrastructure Security Agency Act of 2017.'' I appreciate your support in bringing this legislation before the House of Representatives, and accordingly, understand that the Committee on Transportation and Infrastructure will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Transportation and Infrastructure does not waive any jurisdiction over the subject matter contained in this bill or similar legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee represented on the conference committee. The Committee on Homeland Security will include mutually agreed upon changes to the legislation into the bill prior to floor consideration.

I will insert copies of this exchange in the report on the bill and in the Congressional Record during consideration of this bill on the House floor. I thank you for your cooperation in this matter.

Sincerely,

MICHAEL T. MCCAUL,
Chairman.

Ms. BARRAGÁN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017.

Mr. Speaker, H.R. 3359 would make long-overdue organizational changes within the Department of Homeland Security's National Protection and Programs Directorate, otherwise known as NPPD.

I am a strong supporter of this measure that seeks to empower the DHS to carry out one of its most important and difficult missions: helping Federal agencies and critical infrastructure owners and operators secure themselves against physical and cyber attacks.

Importantly, it would rename NPPD the Cybersecurity and Infrastructure Security Agency, or CISA, to better communicate its mission to stakeholders, agency partners, and the cyber talent the DHS needs to come work in the Federal Government.

Now, make no mistake, these are not mere administrative or bureaucratic changes. H.R. 3359 would transform NPPD into an operational agency on par with the TSA or Customs and Border Protection.

It seems that, with each passing day, we learn of new ways adversaries and cyber criminals are looking to exploit the cyber weaknesses of Federal agencies and our Nation's critical infrastructure. Last year, we found ourselves in uncharted territory when we learned that our electoral system was under attack by one of the world's most sophisticated cyber actors: the Russian Government.

Now, to respond to these evolving cyber threats, Congress has put its faith in the DHS; and, in turn, the DHS looks to NPPD, a small, under-resourced headquarters component established a decade ago to carry out a far more limited mission than the one it has today.

Over the past few years, Congress has expanded NPPD's cyber authorities and responsibilities without elevating NPPD's standing commensurate with its growing mission.

Further, as NPPD has gotten better at delivering cybersecurity assistance and other services to public and private sector partners, it has seen a surge in demand for its services. For example, in the wake of the Russian efforts to hack the 2016 Presidential election, State and local elected officials are now requesting DHS cybersecurity services.

Secretaries of Homeland Security came to us during the Obama administration, and now under the Trump administration, to ask for our help in organizing the Directorate into an operational cybersecurity agency. It is time we grant this request.

Reorganizing and rebranding NPPD should enhance the DHS' standing with respect to its Federal and international peers, clarify its organizational mission, and boost workforce morale. Our expectation is that, with higher moral and mission clarity, the DHS will be able to better compete with the private sector and Federal agencies, like the NSA and the CIA, for a short supply of talented cyber professionals.

Finally, CISA will be in a better position to carry out its core cybersecurity and infrastructure protection activities, like risk and vulnerability assessments for hospitals, banks, the electrical grid, and now election systems. We need NPPD to carry out these activities swiftly, effectively, and in a way that respects privacy and civil liberties; and we cannot expect it to work with one hand tied behind its back.

This bill is the result of bipartisan negotiations, and I want to thank Chairman MCCAUL and Chairman RATCLIFFE for their commitment to see this through and working collaboratively to get this done.

Mr. Speaker, I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield 5 minutes to the distinguished gentleman from Texas (Mr. RATCLIFFE), the chairman of the Subcommittee on Cybersecurity and Infrastructure Protection.

Mr. RATCLIFFE. Mr. Speaker, I rise today in support of the Cybersecurity and Infrastructure Security Agency Act of 2017.

Mr. Speaker, we are here today to take action on what I believe is the defining public policy challenge of our generation: the cybersecurity posture of the United States.

We have seen cyber attacks hit every sector of our economy with devastating impacts to both government agencies and to the private sector alike. It is our duty to ensure that we are doing our very best to defend against the very real threats that our cyber adversaries now pose.

The Department of Homeland Security is the Federal Government's lead civilian agency for cybersecurity. Within it, the National Protection and Programs Directorate, or NPPD, leads our national effort to safeguard and to enhance the resilience of our Nation's physical and cyber infrastructure, helping Federal agencies and, when requested, also helping the private sector to harden their networks and to respond to cybersecurity incidents.

As the cyber threat landscape continues to evolve, Mr. Speaker, so should the Department of Homeland Security. H.R. 3359 elevates the cybersecurity and the infrastructure security missions of NPPD to strengthen the Federal Government's ability to act and react to the changing threat landscape.

The cybersecurity mission today is extremely challenging due to a number of factors: the ability of malicious actors to operate from anywhere in the world now, the linkages between cyberspace and our physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

The Cybersecurity and Infrastructure Security Act of 2017 rises to this challenge and prioritizes the Department of Homeland Security's vital role in cyberspace. By authorizing the Cybersecurity and Infrastructure Security Agency within the DHS, this bill establishes the structure, the nomenclature, and the flexibility to best serve the American people.

The Cybersecurity and Infrastructure Security Agency will be structured to best work with partners at all levels of government, from the private and the nonprofit sectors, to share information and to build greater trust in order to make our cyber and our physical infrastructure more secure.

This bill provides the necessary overarching structure and the interdepartmental flexibility to best allow the DHS to execute its mission in both cybersecurity and the infrastructure security space.

Mr. Speaker, we consider this legislation at a great time of transition and opportunity for the DHS. Just last week, Kirstjen Nielsen was sworn in as the Secretary of Homeland Security. In addition to an impressive record of public service, Secretary Nielsen brings unprecedented cybersecurity experience and savvy to the agency, qualifications fitting the threat landscape that she now inherits.

□ 1645

We owe it to her and to the dedicated women and men working alongside her to ensure that DHS has the proper organization and resources to carry out its mission as the lead civilian cybersecurity agency in our Federal Government.

Mr. Speaker, I want to thank Chairman MCCAUL for his leadership and his dogged determination in this effort and getting this bill to the floor, as well as the other committees of jurisdiction who worked closely to craft this compromise.

Mr. Speaker, the cybersecurity challenges we face are about more than protecting bottom lines or intellectual property or even our Nation's most sensitive classified information. Ultimately, our obligation as lawmakers to be protective cybersecurity stewards stems from a fundamental obligation to safeguard the American people. This is what we aim to do with this legislation, and I urge my colleagues to join me in supporting it.

Ms. BARRAGÁN. Mr. Speaker, I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield 1 minute to the gentleman from Wisconsin (Mr. GALLAGHER).

Mr. GALLAGHER. Mr. Speaker, I rise today in support of H.R. 3359, of which I am a proud cosponsor.

This bill provides an updated framework to reorganize and grant additional authorities to the Department of Homeland Security's cybersecurity and infrastructure protection missions.

Currently, the National Protection and Programs Directorate has responsibility for overseeing the Department's cyber roles; and while DHS has come a long way since inception in 2002, the rapid adaptation of threats in cyberspace demands that we continue to look for ways to evolve and demands that we who oversee this are more nimble and that we can adapt accordingly and keep outpacing our adversaries.

As we have seen, Russia, China, Iran, and various nonstate actors have all demonstrated a willingness to penetrate American networks. We have had high-ranking military officials in our military claim that we are already outgunned in cyberspace right now, and it is up to us to sound the alarm and make sure that we are staying ahead of our adversaries.

Mr. Speaker, I am proud to be part of that effort. I salute the chairman; and, given the Department of Homeland Security's central role in protecting the Federal Government's civilian networks, it is imperative that Congress, through its oversight role, ensures that the men and women at DHS have all the legal authorities they need to carry out this mission.

Mr. Speaker, this bill has been a priority of the Homeland Security Committee for several years, and I want to acknowledge the chairman for his continued leadership on this issue.

Ms. BARRAGÁN. Mr. Speaker, I reserve the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield 2 minutes to the gentleman from Louisiana (Mr. HIGGINS).

Mr. HIGGINS of Louisiana. Mr. Speaker, I rise today in support of H.R. 3359, the Cybersecurity and Infrastructure Security Agency Act of 2017, authored by my colleague, Homeland Security Committee Chairman MCCAUL. I am an original cosponsor of this bill.

Mr. Speaker, America faces a new, emerging peril: threats to our cyber systems and networks. This bill calls for the authorization of a designated cybersecurity agency within DHS by retasking the National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency. This change will allow DHS to provide specific focus on the ever-increasing cyber threats that face our Nation. This bill will help to ensure that the United States can respond to any attack against our Nation's cyber assets.

Mr. Speaker, I thank Chairman MCCAUL for his work on crafting this important piece of legislation, and I urge all my colleagues on both sides of the aisle to support its passage.

Ms. BARRAGÁN. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, H.R. 3359 has broad support on both sides of the aisle.

We talk a lot about the need to harden our cyber defenses against an evolving array of virtual threats. Reorganizing and rebranding NPPD as the

Cybersecurity and Infrastructure Security Agency has the potential of enhancing DHS' cybersecurity capacity, boosting morale, and bringing its critical infrastructure protection workforce together in an unprecedented way.

As an operational agency, CISA will be positioned to foster better collaboration between the cyber and physical sides of the house, bringing its cybersecurity analysts together with chemical inspectors, protective security advisers, emergency communication specialists, and Federal Protective Service officers for a more holistic approach to critical infrastructure protection.

Mr. Speaker, mapping out a new agency is a complicated task, but this measure is long overdue. I urge my colleagues to support this bipartisan legislation, and I yield back the balance of my time.

Mr. MCCAUL. Mr. Speaker, I yield myself the balance of my time.

Mr. Speaker, I cannot go into the classified space in this setting, but I can tell you that our foreign adversaries are looking to hurt us and hit us every day, whether it be from Russia, from China, from Iran, from North Korea. The attacks have targeted Home Depot, Sony, Equifax, 20 million security clearances stolen, to other reports that I can't even get into. But it is a serious threat.

When people ask me what keeps me up at night, of course ISIS does and of course al Qaida does. What happened today in New York, I was just there this morning when the bomb went off. But a cyber attack could bring down our power grid, could bring down our stock market, our financial institutions, our energy sector. A major cyber attack on this Nation could cripple this Nation and its economy and the lives of the people in the United States. Mr. Speaker, that is why this bill is so important, to elevate the civilian agency within the Department, to form a single agency that deals with cybersecurity.

I am very proud of the work my colleagues have done to get to this point. I have been, as Mr. RATCLIFFE said, very dogged in my determination, and I would urge that the Senate take up this measure because we cannot afford to delay because the threat is that great.

Mr. Speaker, I yield back the balance of my time.

Mr. LANGEVIN. Mr. Speaker, let me begin by thanking Chairman MCCAUL and Ranking Member THOMPSON for their dedication to improving our cybersecurity posture. Since the Chairman and I founded the Congressional Cybersecurity Caucus together nearly a decade ago, I have come to firmly believe that cybersecurity is the national and economic security challenge of the 21st Century, and both Congress and the executive branch must take steps to recognize and mitigate the risks we face in our hyper-connected society. Thanks to the leadership of the Chairman and Ranking Member, the Committee on Homeland Security has consistently been at the forefront on these issues, and while much remains to be done, we are worlds away from when I originally took the cyber subcommittee gavel in 2007. The bill we have before us today is a testament to those efforts, and I strongly support this latest iteration of CISA to reorganize the National Protection and Programs Directorate (NPPD) and enhance the capabilities and the profile of DHS's cybersecurity activities.

As one of its core missions, DHS is charged with helping Federal agencies and critical infrastructure owners and operators secure themselves against physical and cyber attacks. For the past decade, that mission has been carried out by NPPD, a small headquarters component of the Department. Since its establishment, NPPD's role in defending the nation and the .gov domain from cyber intrusions has grown in concert with the increasing threat to our networks.

It's a growth that the Committee—and the Congress as a whole—has recognized and encouraged, with the passage of laws including the National Cybersecurity Protection Act of 2014, which authorized the National Cybersecurity and Communications Integration Center, and the Cybersecurity Act of 2015, which made NPPD the federal government's primary hub for cyber threat indicator sharing. Today, NPPD is home to two of the premiere computer security incident response teams in the world and has been recognized as the whole-of-government asset response lead in the National Cyber Incident Response Plan. It also continues to lead efforts in protecting federal networks through the Federal Network Resilience Division, which assists other agencies with risk management, guides enterprise security policy, and implements programs like Continuous Diagnostics and Mitigation and EINSTEIN.

NPPD is clearly acting in an operational capacity today, but despite this fact, Congress has not yet elevated NPPD's standing to be commensurate with these added responsibilities. H.R. 3359 acknowledges the evolution of the component by transforming NPPD into an operational agency on par with TSA or Customs and Border Protection. As part of the reorganization, NPPD will be renamed the ''Cybersecurity and Infrastructure Security Agency,'' or CISA, to accurately reflect its role.

This restructuring was the top legislative priority of DHS Secretary Jeh Johnson before he left office, and I am grateful that Secretary Kelly took up the mantle in the new Administration.

Bringing clarity with the new agency structure also stands to benefit the many cyber defenders working tirelessly at the Department to keep us safe. I have often said that all of the risk mitigation policies and intrusion detection systems in the world are nothing without a skilled workforce. Congress and the Department have been working jointly to reduce the shortage of cybersecurity analysts at NPPD, and it is my hope that an empowered Cybersecurity and Infrastructure Security Agency will be able to compete for the best cyber talent. After all, what mission is more exciting than protecting your fellow Americans from the canniest of adversaries attempting to do us harm in this new domain? I hope that all of the young people considering a career in this emerging field—young people like the brilliant CyberCorps students I enjoy speaking with—will look at Congress's support for DHS's cybersecurity work and jump at the opportunity to be in the vanguard at this new agency.

Mr. Speaker, I also want to speak about the important clarity H.R. 3359 brings to a broader policy debate that has been kicking around Washington, DC, for some time now.

I serve on the House Armed Services Committee, where I am privileged to act as Ranking Member of the Subcommittee on Emerging Threats and Capabilities. In this role, I oversee United States Cyber Command, and I have the utmost respect for the service members in uniform defending our country in the digital domain. I have also had the privilege to serve on the Permanent Select Committee on Intelligence, where I heard weekly about the all-too-often unsung heroes of our Intelligence Community and their efforts to protect our national interests in cyberspace.

I say this, Mr. Speaker, because I want to be clear that I have a deep understanding of and appreciation for our military and intelligence services' cybersecurity prowess.

But I also believe that the powers and authorities of those entities are rightly constrained when it comes to domestic activities. Protecting our domestic cyber assets in peacetime needs to be the responsibility of a civilian organization, and that organization is the Cybersecurity and Infrastructure Security Agency created under this bill. We saw this debate play out during consideration of the Cybersecurity Information Sharing Act of 2015, where it was also decided in favor of a civilian hub, the NCCIC that is at the heart of NPPD. I hope passage of H.R. 3359 will help move the debate on from where authorities should be housed and instead focus on the operationalization of said authorities.

Mr. Speaker, as I mentioned at the outset, this bill owes its existence to the collaborative efforts of Chairman MCCAUL and Ranking Member THOMPSON. But it also reflects the bipartisan spirit of two of my good friends who head the Subcommittee on Cybersecurity and Infrastructure Protection, Mr. RATCLIFFE and Mr. RICHMOND. And, like any effort of this body, it owes a great deal to the staff who work tirelessly behind the scenes supporting our efforts. In particular, I would like to Kirsten Duncan and Moira Bergin, the Majority and Minority staff directors for the Cyber Subcommittee for helping to get this bill to the Floor. And I would also like to thank their predecessors, Brett DeWitt and Chris Schepis, for laying the groundwork for its consideration this Congress.

This bill is important. It's bipartisan. And it's overdue. I hope my colleagues will join me in supporting this important measure, and I hope the Senate moves swiftly to pass it through their Chamber.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Texas (Mr. MCCAUL) that the House suspend the rules and pass the bill, H.R. 3359, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

SECURING GENERAL AVIATION AND COMMERCIAL CHARTER AIR CARRIER SERVICE ACT OF 2017

Mr. ESTES of Kansas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3669) to improve and streamline security procedures related to general aviation and commercial charter air carrier utilizing risk-based security standards, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3669

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Securing General Aviation and Commercial Charter Air Carrier Service Act of 2017''.

SEC. 2. WEB-BASED SECURE FLIGHT COST AND FEASIBILITY STUDY.

Not later than 120 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a study to determine the cost and feasibility of establishing web-based access to Secure Flight for commercial charter air carriers.

SEC. 3. SCREENING IN AREAS OTHER THAN PASSENGER TERMINALS.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration is authorized to provide screening services to a commercial charter air carrier in areas other than primary passenger terminals of airports upon the request of such carrier.

(b) REQUEST.—A commercial charter air carrier that wants screening services to be provided to such carrier in an area other than a primary passenger terminal shall request the Federal Security Director for the airport at which such services are requested.

(c) AVAILABILITY.—A Federal Security Director may elect to provide screening services under this section if such services are available.

(d) AGREEMENTS.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall enter into an agreement with a commercial charter air carrier for compensation from such carrier requesting the use of screening services under this section for all reasonable costs in addition to overtime costs that are incurred in the provision of such services.

(2) AVAILABILITY.—Any compensation received by the Transportation Security Administration pursuant to an agreement under this subsection shall be credited to the account used in connection with the provision of the screening services that are the subject of such agreement, notwithstanding section 3302 of title 31, United States Code.

SEC. 4. REPORT ON GENERAL AVIATION SECURITY AND SELECT AVIATION SECURITY TOPICS.

Not later than 120 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the Aviation Security Advisory Committee, shall, consistent with the requirements of paragraphs (6) and (7) of section 44946(b) of title 49, United States Code, submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate an implementation plan, including an implementation schedule, for any of the following recommendations that were adopted by the Aviation Security Advisory Committee and with which the Administrator has concurred before the date of the enactment of this Act:

(1) The recommendation regarding general aviation access to Ronald Reagan Washington National Airport, as adopted on February 17, 2015.

(2) The recommendation regarding the vetting of persons seeking flight training in the United States, as adopted on July 28, 2016.

(3) Any other such recommendations relevant to the security of general aviation adopted before the date of the enactment of this Act.

SEC. 5. DESIGNATED STAFFING FOR GENERAL AVIATION.

The Administrator of the Transportation Security Administration is authorized to designate not fewer than one full time employee of the Administration to be responsible for engagement with general aviation stakeholders and manage issues related to general aviation.

SEC. 6. SECURITY ENHANCEMENTS.

Not later than one year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the Aviation Security Advisory Committee, shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the feasibility of requiring security threat assessments for all candidates seeking flight school training in the operation of any aircraft having a maximum certificated takeoff weight of more than 12,500 pounds to further enhance the vetting of persons seeking such training in the United States.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Kansas (Mr. ESTES) and the gentlewoman from California (Ms. BARRAGÁN) each will control 20 minutes.

The Chair recognizes the gentleman from Kansas.

GENERAL LEAVE

Mr. ESTES of Kansas. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Kansas?

There was no objection.

Mr. ESTES of Kansas. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I am honored to represent the Fourth District of Kansas. My hometown, Wichita, Kansas, is proud to be known as The Air Capital of the World.

Over 100 years ago, Clyde Cessna began manufacturing planes outside of Wichita. Since then, Wichita has grown to be the leading center for aviation manufacturing around the world. In fact, 67 percent of the world's embedded general aviation fleet is manufactured in Kansas. We are proud of the work we do in Wichita, and general aviation has a good home in Kansas.

I worked for many years in the general aviation industry as a process improvement engineer. That is why I am putting forward this important piece of legislation that will help ensure general aviation remains safe and secure.

Mr. Speaker, I urge my colleagues to vote for H.R. 3669, the Securing General Aviation and Commercial Charter Air Carrier Service Act.

General aviation, which includes all noncommercial flights and commercial charters, accounts for nearly two-thirds of all towered operations in the United States. This does not account for the thousands of untowered operations in the United States that are only served by the general aviation community.

However, general aviation and commercial charter air service represent a small fraction of TSA's stakeholder community, causing their issues and concerns to fall to the bottom of the agency's priorities. This bill seeks to elevate some of these important but often overlooked security issues. The general aviation community has important safety concerns that deserve to be heard and acted upon by TSA.

Commercial charters are forced to use antiquated and unsecure systems to ensure their passengers' safety. Currently, the software needed to connect to TSA's Secure Flight system for vetting passengers costs tens of thousands of dollars. Commercial airlines serving 2½ million passengers a day can easily adopt the software; However, smaller operators do not have the passenger volume to absorb the cost.

Currently, TSA emails commercial charter operators large datasets in spreadsheet format that their operators must then check against passenger manifests. This unsecure method presents a serious security risk for this data, which could include sensitive personal information.

I have heard from commercial charter operators that access to the Secure Flight system is a top priority so that they can ensure the safety of the airspace and their passengers. TSA should explore creating a web-based program that these operators could access that would have realtime passenger vetting information and would prevent the unintended distribution of sensitive security information.

Currently, private charter air carriers must use their own flight crews or private screening companies to screen passengers. In certain instances, these carriers would like to occasionally use on- or off-duty TSA agents to screen passengers due to the expertise and training that these agents possess. However, when private charters are performed on short notice, carriers are unable to bring off-duty TSA screeners into their own program due to certain FAA regulations. Language in this bill would allow private charters the flexibility to request and pay for this service without cost to the taxpayer.

Additionally, the Aviation Security Advisory Committee has approved several recommendations regarding improvements to security rules and regulations for general aviation and commercial charter air carrier programs. These important recommendations have yet to be implemented by TSA. This legislation requires TSA to develop an implementation plan and